Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): 1033-T00534

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on 12-11-06

Signature: Jeaneaux Jordan

Typed or printed name: Jeaneaux Jordan

Application Number	Filed
10/634,117	August 4, 2003

First Named Inventor: James M. Doherty, et al.

Art Unit	Examiner
2136	HOANG, Daniel L.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 38,342.
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

Signature

Jeffrey G. Toler
Typed or printed name

512-327-5515
Telephone number

12-11-2006
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	James M. Doherty et al.		
Title:	HOST INTRUSION DETECTION AND ISOLATION		
App. No.:	10/634,117	Filed:	August 4, 2003
Examiner:	HOANG, Daniel L.	Group Art Unit:	2136
Customer No.:	60533	Confirmation No.:	5753
Atty. Dkt. No.:	1033-T00534		

Mail Stop AF
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

REMARKS IN SUPPORT OF THE PRE-APPEAL BRIEF REQUEST FOR REVIEW

Dear Sir:

In response to the Final Office Action mailed on October 18, 2006 (hereinafter, "the Final Office Action"), Applicants file herewith a Notice of Appeal and a Pre-Appeal Brief Request for Review and request review of the following issues:

1. Claims 1, 3-13, 15, and 17-27 Are Allowable Over Douglas and Mann

Applicants traverse the rejection of claims 1, 3-13, 15, and 17-27 under 35 U.S.C.§103(a) over U.S. Patent Publication No. 2004/0049693 ("Douglas") in view of U.S. Patent No. 6,081,894 ("Mann") at page 3 of the Final Office Action. The Final Office Action acknowledges that Douglas does not disclose or suggest, in response to detecting an intrusion event, isolating at least one network interface from a computer network and taking a host system down to a single user state so that access to the host computer system is limited to physical access at the host computer system, as recited by independent claims 1 and 15.

CERTIFICATE OF TRANSMISSION/MAILING
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to the Commissioner for Patents on 12-11-06.

Jeaneaux Jordan
Typed or Printed Name

Signature

The Final Office Action asserts that Mann discloses this feature, citing Mann at col. 3, lines 2-5. However, Mann discloses that the data sending entity is isolated from the data receiving entity without disrupting normal operation of either entity. *See Mann*, col. 2, lines 30-32 (emphasis added). At the section referenced by the Final Office Action, Mann states:

> When a virus is detected, a data isolator 60, that is responsive to a control signal 42 from the data comparator 40, isolates the first data channel 22 from the second data channel 32. Thus, viruses are detected and prevented from being received by the data receiving entity 30.

Mann, col. 3, lines 2-5. Thus, the data isolator of Mann resides between the data receiving entity (e.g., personal computer or local area network) and the data sending entity (i.e. the internet). *See Mann*, col. 2, line 61 through col. 3, line 7.

Applicants note that claims 1 and 15 recite "operating the host computer in a multi-user mode" and "a host computer system to operate in a multi-user mode," respectively. Additionally, independent claims 1 and 15 recite "in response to detecting the intrusion event, isolating the at least one network interface from the computer network and taking the host computer system down to a single user state so that access to the host computer system is limited to physical access at the host computer system." The "single user state" is a different state from normal operation ("multi-user mode"). Thus, Mann does not disclose or suggest taking the host computer system down to a single user state, as recited by independent claims 1 and 15.

The Final Office Action states:

> When the first data channel is isolated from the second data channel, it is obvious that the two entities are isolated from each other. Because there are only two entities and they are isolated from each other, it is clear that both entities are in single user states.

The Final Office Action, p. 2.

The assumption that "it is clear that both entities are in single user states" is incorrect and not applicable, since the receiving entity was never indicated to be in a multi-user state. Moreover, the data sending entity is indicated to be the Internet (*See Mann*, col. 2, lines 62-63), so it is unclear how the data sending entity could ever be reduced to a single user state.

Further, Mann discloses that the isolation is provided without disrupting normal operation. *See Mann*, col. 2, lines 30-32. In direct contrast, claims 1 and 15 recite "taking the host computer system down to a single user state." Altering the state of the device from a multi-user state to a single user state is a disruption of normal operation. Thus, Mann teaches away from claims 1 and 15.

Moreover, Mann discloses that the data receiving entity may be a personal computer or a local area network. *See Mann*, col. 2, lines 63-64. Mann provides no indication that the personal computer operates in a multi-user mode and provides no indication that the data isolator is adapted to take the receiving device down to a single user state. When the receiving device is a local area network, it is unclear how the local area network may be reduced to a single user state without disruption of normal operation. Further, Mann does not disclose or suggest any direct action taken with respect to the data receiving entity. Instead, Mann discloses that the data isolator isolates the data receiving entity by isolating a first data channel (extending from the data sending entity to the data isolator) from a second data channel (extending from the data isolator to the data receiving device). *See Mann*, Abstract, and col. 2, line 61 through col. 3, line 5.

Thus, Mann does not disclose or suggest "taking the host computer system down to a single user state," as recited by claims 1 and 15. Therefore, Mann fails to overcome the deficiencies of Douglas, and the asserted combination of Douglas and Mann fails to disclose or suggest each and every element of independent claims 1 and 15, and of dependent claims 3-13 and 17-27, at least by virtue of their dependency from one of claims 1 and 15. At least for the foregoing reasons, the rejection of claims 1, 3-13, 15, and 17-27 should be withdrawn.

2. *Claim 14 Is Allowable Over Douglas and Mann*

Applicants traverse the rejection of claim 14 under 35 U.S.C. §103(a) over Douglas in view of Mann at pages 3 and 6 of the Final Office Action. None of the cited references, alone or in combination, recite the particular arrangement of features recited by independent claim 14.

Claim 14 recites in response to detecting the intrusion event, the method includes issuing an IFCONFIG down command to the at least one network interface to isolate the at least one network interface from the computer network, issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to a single user state, and writing a log of the intrusion event to a log database that is not located on the second computer system.

The Final Office Action rejects claim 14 over Douglas and Mann as applied to claims 1-8 and 10. *See the Final Office Action*, p. 6. As previously discussed, Douglas fails to disclose or suggest, in response to detecting an intrusion event, taking the host computer down to a single user state. Also, as previously discussed, Mann provides no indication that the personal computer operates in a multi-user mode and provides no indication that the data isolator is adapted to take the receiving device down to a single user state. Moreover, Mann does not disclose or suggest issuing an INIT1 command to an operating system of the host computer system to take the host computer system down to a single user state, as recited by claim 14. Instead, Mann provides isolating by isolating the first data channel from the second data channel. *See Mann*, Abstract, and col. 2, line 61 through col. 3, line 5. Thus, the asserted combination of Douglas and Mann fails to disclose or suggest at least one element of independent claim 14. Therefore, the rejection of claim 14 should be withdrawn.

CONCLUSION

Applicants have pointed out specific features of the claims not disclosed, suggested or rendered obvious by the references applied in the Final Office Action. Accordingly, Applicants respectfully request reconsideration and withdrawal of each of the objections and rejections, as well as an indication of allowability of each of the claims now pending.

The Commissioner is hereby authorized to charge any fees, which may be required, or credit any overpayment, to Deposit Account Number 50-2469.

Respectfully submitted,

12-11-2006
Date

Jeffrey G. Toler, Reg. No. 38,342
Attorney for Applicant(s)
TOLER SCHAFFER, L.L.P.
5000 Plaza On The Lake, Suite 265
Austin, Texas 78746
(512) 327-5515 (phone)
(512) 327-5575 (fax)

JGT/RMR